AFRL-OSR-VA-TR-2013-0495

(MURI-08) COLLABORATIVE POLICIES AND ASSURED INFORMATION SHARING

ANUPAM DATTA

LELAND STANFORD JUNIOR UNIVERSITY

09/12/2013
Final Report

DISTRIBUTION A: Distribution approved for public release.

AIR FORCE RESEARCH LABORATORY
AF OFFICE OF SCIENTIFIC RESEARCH (AFOSR)/RSL
ARLINGTON, VIRGINIA 22203
AIR FORCE MATERIEL COMMAND

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
09/10/2013

2. REPORT TYPE
Final

3. DATES COVERED *(From - To)*
June 2008-May 2013

4. TITLE AND SUBTITLE
(MURI-08) Collaborative Policies and Assured Information Sharing

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-08-1-0352

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Anupam Datta

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213-3815

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AF Office of Scientific Research
875 N. Randolph St. Room 3112
Arlington, VA 22203
Patricia S Gorski

10. SPONSOR/MONITOR'S ACRONYM(S)
USAF, AFRL

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
SF298

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A - Approved for Public Release

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not construed as an official US/

14. ABSTRACT

Privacy has become a significant concern in modern society as personal information about individuals is increasingly collected, used, and shared, often using digital technologies, by a wide range of organizations. To mitigate privacy concerns, organizations are required to respect privacy laws in regulated sectors (e.g., HIPAA in healthcare, GLBA in financial sector) and to adhere to self-declared privacy policies in self-regulated sectors (e.g., privacy policies of companies such as Google and Facebook in Web services). We investigate the possibility of formalizing and enforcing such practical privacy policies using computational techniques. We formalize privacy policies that prescribe and proscribe flows of personal information. Recognizing that traditional preventive access control and information flow control mechanisms are inadequate for enforcing such privacy policies, we develop principled audit and accountability mechanisms that seek to encourage policy-compliant behavior by detecting policy violations, assigning blame, and punishing violators. We apply these techniques to several U.S. privacy laws and organizational privacy policies, in particular, producing the first complete logical specification and audit of all disclosure-related clauses of the HIPAA Privacy Rule.

15. SUBJECT TERMS
Privacy Protection, Audit Mechanisms, Accountability Mechanisms, HIPAA Privacy Rule

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Anupam Datta
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	UU	3	**19b. TELEPHONE NUMBER** *(include area code)* 412-268-4254

AFOSR MURI: Collaborative Policies and Assured Information Sharing

CMU PI: Anupam Datta

Dated: September 11, 2013

Report:

Privacy has become a significant concern in modern society as personal information about individuals is increasingly collected, used, and shared, often using digital technologies, by a wide range of organizations. To mitigate privacy concerns, organizations are required to respect privacy laws in regulated sectors (e.g., HIPAA in healthcare, GLBA in financial sector) and to adhere to self-declared privacy policies in self-regulated sectors (e.g., privacy policies of companies such as Google and Facebook in Web services). We investigate the possibility of formalizing and enforcing such practical privacy policies using computational techniques. We formalize privacy policies that prescribe and proscribe flows of personal information. Recognizing that traditional preventive access control and information flow control mechanisms are inadequate for enforcing such privacy policies, we develop principled audit and accountability mechanisms that seek to encourage policy-compliant behavior by detecting policy violations, assigning blame, and punishing violators. We apply these techniques to several U.S. privacy laws and organizational privacy policies, in particular, producing the first complete logical specification and audit of all disclosure-related clauses of the HIPAA Privacy Rule. In ongoing work with Microsoft Research, Symantec Research Lab, and Illinois Health Information Exchange, we are working on developing these methods further and in applying them in industry settings to provide greater assurance that information sharing appropriately respects privacy expectations and other institutional agreements.

We provide below additional details about the most significant research results below. A complete list of publications is appended at the end.

1. Formalizing the HIPAA Privacy Rule and Gramm-Leach Bliley Act

   Despite the wide array of frameworks proposed for the formal specification and analysis of privacy laws, there has been comparatively little work on expressing large fragments of actual privacy laws in these frameworks. We attempt to bridge this gap by giving the **first complete logical formalizations** of the transmission-related portions of the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). To this end, we develop the PrivacyLFP logic, whose features include support for disclosure purposes, real-time constructs, and self-reference via fixed points. To illustrate these features and demonstrate PrivacyLFP's utility, we present formalizations of a collection of clauses from these laws. We discuss ambiguities in the laws that our formalizations revealed and sketch preliminary ideas for computer-assisted enforcement of such privacy policies.

2. Policy Auditing over Incomplete Logs

We present the design, implementation and evaluation of an algorithm that checks audit logs for compliance with privacy and security policies. The algorithm, which we name reduce, addresses two fundamental challenges in compliance checking that arise in practice. First, in order to be applicable to realistic policies, reduce operates on policies expressed in a first-order logic that allows restricted quantification over infinite domains. We build on ideas from logic programming to identify the restricted form of quantified formulas. The logic can, in particular, express all 84 disclosure-related clauses of the HIPAA Privacy Rule, which involve quantification over the infinite set of messages containing personal information. Second, since audit logs are inherently incomplete (they may not contain sufficient information to determine whether a policy is violated or not), reduce proceeds iteratively: in each iteration, it provably checks as much of the policy as possible over the current log and outputs a residual policy that can only be checked when the log is extended with additional information. We prove correctness, termination, time and space complexity results for reduce. We implement reduce and optimize the base implementation using two heuristics for database indexing that are guided by the syntactic structure of policies. The implementation is used to check simulated audit logs for compliance with the HIPAA Privacy Rule. Our experimental results demonstrate that the algorithm is fast enough to be used in practice.

3. Audit Games for Privacy Protection

   We developed models and mechanisms for accountable data governance that can provide operational guidance to organizations on how to allocate their budget to best manage privacy risks (through audit and punishments) as well as evaluate effectiveness of public policy interventions in promoting privacy-respecting behavior (e.g., HHS audits, data breach disclosure laws). We designed models and algorithms for risk management in healthcare organizations in settings where the adversary's incentives are known (e.g., gain from medical identity theft etc.) and settings in which the adversary's incentives are not known. We used the models to predict effectiveness of public policy interventions, in particular, external audits (e.g., mandated by HHS) and data breach notification laws. A specific result published at IJCAI 2013 is summarized below: Effective enforcement of laws and policies requires expending resources to prevent and detect offenders, as well as appropriate punishment schemes to deter violators. In particular, enforcement of privacy laws and policies in modern organizations that hold large volumes of personal information (e.g., hospitals) relies heavily on internal audit mechanisms. We study economic considerations in the design of these mechanisms, focusing in particular on effective resource allocation and appropriate punishment schemes. We present an audit game model that is a natural generalization of a standard security game model for resource allocation with an additional punishment parameter. Computing the Stackelberg equilibrium for this game is challenging because it involves solving an optimization problem with non-convex quadratic constraints. We present an additive FPTAS that efficiently computes a solution that is arbitrarily close to the optimal solution.

Publications:

1) J. Blocki, N. Christin, A. Datta, A. Procaccia, A. Sinha, Audit Games, in *Proceedings of 23rd International Joint Conference on Artificial Intelligence*, August 2013. [Full Version]
2) J. Blocki, A. Blum, A. Datta, O. Sheffet, Differentially Private Data Analysis of Social Networks via Restricted Sensitivity, in *Proceedings of 4th Innovations in Theoretical Computer Science Conference*, January 2013. [Full Version]
3) J. Blocki, N. Christin, A. Datta, A. Sinha, Audit Mechanisms for Provable Risk Management and Accountable Data Governance, in *Proceedings of 3rd Conference on Decision and Game Theory for Security*, November 2012. [Paper]
4) J. Blocki, A. Blum, A. Datta, O. Sheffet, The Johnson-Lindenstrauss Transform Itself Preserves Differential Privacy, in *Proceedings of 53rd Annual IEEE Symposium on Foundations of Computer Science*, October 2012. [Full Version]
5) A. Datta, D. Sharma, A. Sinha, Provable De-anonymization of Large Datasets with Sparse Dimensions, in *Proceedings of ETAPS Conference on Principles of Security and Trust*, March 2012. [Paper]
6) A. Conley, A. Datta, H. Nissenbaum, D. Sharma, Sustaining both Privacy and Open Justice in the Transition from Local to Online Access to Court Records: A Multidisciplinary Inquiry, *Maryland Law Review*, 71 Md. L. Rev. 772 (2012). [Paper]
    i) (Preliminary version presented at the *2011 Privacy Law Scholars Conference*, June 2011.)
7) A. Datta, J. Blocki, N. Christin, H. DeYoung, D. Garg, L. Jia, D. Kaynar, A. Sinha, Understanding and Protecting Privacy: Formal Semantics and Principled Audit Mechanisms, *7th International Conference on Information Systems Security*, December 2011. [Paper]
   Invited Paper
8) D. Garg, L. Jia, A. Datta, Policy Auditing over Incomplete Logs: Theory, Implementation and Applications, in *Proceedings of 18th ACM Conference on Computer and Communications Security*, October 2011 [Paper] [Full Version]
9) J. Blocki, N. Christin, A. Datta, A. Sinha, Audit Mechanisms for Privacy Protection in Healthcare Environments (Position Paper), in *2nd Usenix Workshop on Health Security and Privacy*, August 2011 [Paper]
10) J. Blocki, N. Christin, A. Datta, A. Sinha, Regret Minimizing Audits: A Learning-Theoretic Basis for Privacy Protection, in *Proceedings of 24th IEEE Computer Security Foundations Symposium*, June 2011 [Paper]
11) M. C. Tschantz, D. Kaynar, A. Datta, Formal Verification of Differential Privacy for Interactive Systems, Extended abstract in *Proceedings of the 27th Annual Conference on Mathematical Foundations of Programming Semantics*, May 2011. Full Version [Paper]
    Invited Paper
12) H. DeYoung, D. Garg, L. Jia, D. Kaynar, A. Datta, Experiences in the Logical Specification of the HIPAA and GLBA Privacy Laws, in *Proceedings of 9th ACM Workshop on Privacy in the Electronic Society*, October 2010. [Paper] [FullVersion]